PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-022647
(43)Date of publication of application : 26.01.2001

(51)Int.CL G06F 12/14
G06F 15/00
G09C 1/00
G11B 20/10
H04L 9/32

(21)Application number : 11-196207
(22)Date of filing : 09.07.1999

(71)Applicant : TOSHIBA CORP
MATSUSHITA ELECTRIC IND CO LTD

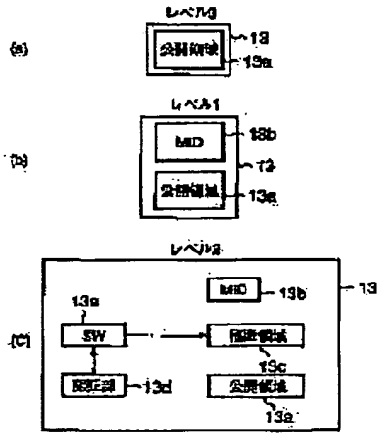
(72)Inventor : KAMIBAYASHI TATSU
KATO HIROSHI
TOMA HIDEYUKI
TATEBAYASHI MAKOTO
HARADA TOSHIHARU
YAMADA HISASHI

(54) METHOD AND DEVICE FOR CONTENTS MANAGEMENT, AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To securely and safely erase contents recorded on a recording medium by decoding an comparing data, used for overwriting on an opposite side, with overwriting data when the data are transferred and confirming that necessary information has been erased when recorded contents are deciphered.

SOLUTION: Overwriting data for erasing information, needed to deciphere contents recorded on a recording medium (MC) 13, by overwriting are deciphered by using 1st common information generated by mutual authentication and then transferred to an opposite side. When data used for overwriting on the opposite side are transferred from the opposite side after being ciphered by using 2nd common information generated by performing mutual authentication again, the data are deciphered with the 2nd common information and then compared with the overwriting data to confirm that the information needed to deciphere the recorded contents has been erased. Where, the MC 13 processes an open area 13a, an identification information storage 13b, a secrecy 13c and an authentication part 13d, etc.



LEGAL STATUS

[Date of request for examination] 19.10.2004

[Date of sending the examiner's decision of rejection]

(19)日本国特許庁（JP）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－22647
（P2001－22647A）
(43)公開日　平成13年1月26日(2001.1.26)

(51)Int.Cl.'	識別記号	FI	テーマコード'(参考)
G06F 12/14	320	G06F 12/14	320E 5B017
15/00	330	15/00	330Z 5B085
G09C 1/00	660	G09C 1/00	660E 5D044
G11B 20/10		G11B 20/10	H 5J104
H04L 9/32		H04L 9/00	675A 9A001

審査請求　未請求　請求項の数6　OL　（全 20 頁）

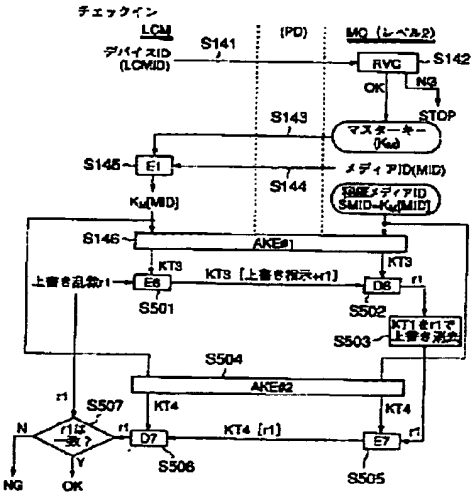
(21)出願番号　特願平11－196207
(22)出願日　平成11年7月9日(1999.7.9)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　上林　逸
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100058479
弁理士　鈴江　武彦　（外５名）

最終頁に続く

(54)【発明の名称】　コンテンツ管理方法およびコンテンツ管理装置および記録媒体

(57)【要約】
【課題】記録媒体に記録された複製コンテンツの消去が確実にしかも安全に行え、記録媒体に記録する複製コンテンツの数の管理が容易にしかも確実に行えるコンテンツ管理方法を提供する。
【解決手段】記録媒体に記録された複製コンテンツを復号する際に必要な情報を上書きすることにより消去するための上書きデータを相互認証により生成された第１の共有情報を用いて暗号化してから相手側に転送し、前記相手側から、再度の相互認証により生成された第２の共有情報を用いて暗号化された該相手側で上書きに用いたデータが転送されてきたら、それを前記第２の共有情報で復号した後、前記上書きデータと比較して前記記録媒体に記録された複製コンテンツを復号する際に必要な情報が消去されたことを確認する。



1

【特許請求の範囲】

【請求項１】 記録媒体に対しコンテンツの記録および消去を行うコンテンツ管理方法において、

前記記録媒体に記録されたコンテンツを復号する際に必要な情報を上書きすることにより消去するための上書きデータを相互認証により生成された第１の共有情報を用いて暗号化してから相手側に転送し、

前記相手側から、再度の相互認証により生成された第２の共有情報を用いて暗号化された該相手側で上書きに用いたデータが転送されてきたとき、それを前記第２の共有情報で復号した後、前記上書きデータと比較して前記記録媒体に記録されたコンテンツを復号する際に必要な情報が消去されたことを確認することを特徴とするコンテンツ管理方法。

【請求項２】 記録媒体に対しコンテンツの記録および消去を行うコンテンツ管理方法において、

前記記録媒体に記録されたコンテンツを復号する際に必要な情報を消去するための指示情報が相互認証により生成された共有情報を用いて暗号化されて相手側から転送された後、再度相互に認証されたとき、前記記録媒体に記録されたコンテンツを復号する際に必要な情報を消去することを特徴とするコンテンツ管理方法。

【請求項３】 記録媒体に対しコンテンツの記録および消去を行うコンテンツ管理装置において、

前記記録媒体に記録されたコンテンツを復号する際に必要な情報を上書きすることにより消去するための上書きデータを相互認証により生成された第１の共有情報を用いて暗号化してから相手側に転送する転送手段と、

前記相手側から、再度の相互認証により生成された第２の共有情報を用いて暗号化された該相手側で上書きに用いたデータが転送されてきたとき、それを前記第２の共有情報で復号した後、前記上書きデータと比較して前記記録媒体に記録されたコンテンツを復号する際に必要な情報が消去されたことを確認する確認手段と、

を具備したことを特徴とするコンテンツ管理装置。

【請求項４】 記録媒体に対しコンテンツの記録および消去を行うコンテンツ管理装置において、

前記記録媒体に記録されたコンテンツを復号する際に必要な情報を消去するための指示情報を相互認証により生成された共有情報を用いて相手側に転送する転送手段と、

この転送手段で指示情報を転送した後、再度相互に認証を行って、前記記録媒体に記録されたコンテンツを復号する際に必要な情報の消去を前記相手側に実行させる消去実行手段と、

を具備したことを特徴とするコンテンツ管理装置。

【請求項５】 演算処理機能を有する記録媒体であって、

相互認証により生成された第１の共有情報を用いて暗号化された、自己に記録されたコンテンツを復号する際に必要な情報を上書きすることにより消去するための上書きデータを相手側より受信したとき、前記第１の共有情報を用いて復号して得られたデータを用いて自己に記録されたコンテンツを復号する際に必要な情報を上書きすることにより消去する消去手段と、

この消去手段で上書きに用いたデータを再度の相互認証により生成された第２の共有情報を用いて暗号化して前記相手側に転送する転送手段と、

を具備したことを特徴とする記録媒体。

【請求項６】 演算処理機能を有する記録媒体であって、

相互認証により生成された共有情報を用いて暗号化された、自己に記録されたコンテンツを復号する際に必要な情報を消去するための指示情報を相手側より受信した後、再度相互に認証されたとき、自己に記録されたコンテンツを復号する際に必要な情報を消去する手段を具備したことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えば、複製コンテンツの数を規制して著作権の保護を図るコンテンツ管理方法およびそれを用いたコンテンツ管理装置に関し、特に、記録媒体に記録された複製コンテンツの消去方法に関する。

【０００２】

【従来の技術】従来、コンテンツ（著作物等）は、コピー管理が行われてきた。コピー世代管理やコピーの数を管理する事により、著作権保護と利用の便宜のバランスをとってきた。

【０００３】さらに、コピー管理に代わって、「移動」の概念が登場してきた。コピーがオリジナルのデータを消去しないのと対照的に、移動は、異なった場所（記録媒体（メディア））にデータを転送すると共に、オリジナルデータを消去する。コンテンツのデジタル化とネットワーク等の普及が、移動によるコピープロテクションが登場した背景にある。

【０００４】

【発明が解決しようとする課題】近年、ネットワーク等を通じたオリジナルに忠実なコピーが可能になったため、コピー管理だけでは、著作権保護が困難になってきた。また、メディアからメディアへの無制限な移動、例えば、データの営利目的の（移動による）配布は、著作権管理を行うことができない。

【０００５】このように、オリジナルのデータ（特に、著作権保護の対象となるようなコンテンツ）の複製を確実に管理することが困難となってきた。

【０００６】特に、著作権保護のため、複製コンテンツの数を規制しながら記録媒体に対し複製コンテンツの記録および消去を行うコンテンツ管理においては、記録媒体に記録された複製コンテンツの移動の際に、当該記録

媒体に記録されている複製コンテンツを確実に消去する必要がある。この場合、複製コンテンツの記録を行う場合とは異なり、その手続の際に、第三者が不正に、例えば複製コンテンツの消去のためのコマンド等を受け取らないよう信号をカット等することにより、容易に当該記録媒体から複製コンテンツの消去を回避することができる。

【０００７】そこで、本発明は、記録媒体に記録する複製コンテンツの数を規制しながら該記録媒体に対しコンテンツの記録および消去を行うコンテンツ管理において、記録媒体に記録されたコンテンツの消去が確実にしかも安全に行えるコンテンツ管理方法およびそれを用いたコンテンツ管理装置および記録媒体を提供することを目的とする。

【０００８】

【課題を解決するための手段】（１）本発明のコンテンツ管理方法（請求項１）は、記録媒体に対しコンテンツの記録および消去を行うコンテンツ管理方法において、前記記録媒体に記録されたコンテンツを復号する際に必要な情報を上書きすることにより消去するための上書きデータを相互認証により生成された第１の共有情報を用いて暗号化してから相手側に転送し、前記相手側から、再度の相互認証により生成された第２の共有情報を用いて暗号化された該相手側で上書きに用いたデータが転送されてきたら、それを前記第２の共有情報で復号した後、前記上書きデータと比較して前記記録媒体に記録されたコンテンツを復号する際に必要な情報が消去されたことを確認することを特徴とする。

【０００９】また、本発明のコンテンツ管理装置（請求項３）は、記録媒体に対しコンテンツの記録および消去を行うコンテンツ管理装置において、前記記録媒体に記録されたコンテンツを復号する際に必要な情報を上書きすることにより消去するための上書きデータを相互認証により生成された第１の共有情報を用いて暗号化してから相手側に転送する転送手段と、前記相手側から、再度の相互認証により生成された第２の共有情報を用いて暗号化された該相手側で上書きに用いたデータが転送されてきたら、それを前記第２の共有情報で復号した後、前記上書きデータと比較して前記記録媒体に記録されたコンテンツを復号する際に必要な情報が消去されたことを確認する確認手段とを具備したことを特徴とする。

【００１０】本発明の記録媒体（請求項５）は、演算処理機能を有する記録媒体であって、相互認証により生成された第１の共有情報を用いて暗号化された、自己に記録されたコンテンツを復号する際に必要な情報を上書きすることにより消去するための上書きデータを相手側より受信したとき、前記第１の共有情報を用いて復号して得られたデータを用いて自己に記録されたコンテンツを復号する際に必要な情報を上書きすることにより消去する消去手段と、この消去手段で上書きに用いたデータを

再度の相互認証により生成された第２の共有情報を用いて暗号化して前記相手側に転送する転送手段とを具備したことを特徴とする。

【００１１】上記本発明によれば、例えば、第三者によるコンテンツの消去のためのコマンド等を受け取らないようにする攻撃を確実に回避することができ、記録媒体に記録されたコンテンツの消去が確実にしかも安全に行え、記録媒体に記録するコンテンツの数の管理が容易にしかも確実に行える。

【００１２】（２）本発明のコンテンツ管理方法（請求項２）は、記録媒体に対しコンテンツの記録および消去を行うコンテンツ管理方法において、前記記録媒体に記録されたコンテンツを復号する際に必要な情報を消去するための指示情報が相互認証により生成された共有情報を用いて暗号化されて相手側から転送された後、再度相互に認証されたとき、前記記録媒体に記録されたコンテンツを復号する際に必要な情報を消去することを特徴とする。

【００１３】本発明のコンテンツ管理装置（請求項４）は、記録媒体に対しコンテンツの記録および消去を行うコンテンツ管理装置において、前記記録媒体に記録されたコンテンツを復号する際に必要な情報を消去するための指示情報を相互認証により生成された共有情報を用いて相手側に転送する転送手段と、この転送手段で指示情報を転送した後、再度相互に認証を行って、前記記録媒体に記録されたコンテンツを復号する際に必要な情報の消去を前記相手側に実行させる消去実行手段とを具備したことを特徴とする。

【００１４】本発明の記録媒体（請求項６）は、演算処理機能を有する記録媒体であって、相互認証により生成された共有情報を用いて暗号化された、自己に記録されたコンテンツを復号する際に必要な情報を消去するための指示情報を相手側より受信した後、再度相互に認証されたとき、自己に記録されたコンテンツを復号する際に必要な情報を消去する手段を具備したことを特徴とする。

【００１５】上記本発明によれば、例えば、第三者によるコンテンツの消去のためのコマンド等を受け取らないようにする攻撃を確実に回避することができ、記録媒体に記録されたコンテンツの消去が確実にしかも安全に行え、記録媒体に記録するコンテンツの数の管理が容易にしかも確実に行える。

【００１６】

【発明の実施の形態】以下、本発明の一実施形態について図面を参照して説明する。

【００１７】図１は、本実施形態にかかる記録媒体（メディア）に記録できる複製コンテンツの数を規制し、メディアへの複製コンテンツの記録、メディアに記録された複製コンテンツの再生等を行う音楽コンテンツ利用管理システム（以下、簡単にＬＣＭと呼ぶことがある）１

の構成例を示したものである。なお、ここでは、コンテンツとして音楽を一例として用いているが、この場合に限らず、映画や、ゲームソフト等であってもよい。また、メディアとしてメモリカード（ＭＣ）を用いているが、この場合に限るものではなく、フロッピーディスク、ＤＶＤ等の各種記録媒体であってもよい。

【００１８】ＥＭＤ（Electronic Music Distributor）は、音楽配信サーバまたは音楽配信放送局である。

【００１９】コンテンツ利用管理システム１は、例えば、パソコン（ＰＣ）であり、複数のＥＭＤ（ここでは、ＥＭＤ＃１～＃３）に対応した受信部＃１～＃３を具備しており、ＥＭＤが配信する暗号化コンテンツまたはそのライセンス（利用条件と暗号化コンテンツの復号鍵Ｋｃ）などを受信する。受信部＃１～＃３は、再生機能や課金機能を有していても良い。配信された音楽コンテンツを試聴するために再生機能が用いられる。又、課金機能を利用して、気に入ったコンテンツを購入する事が可能である。

【００２０】ＬＣＭ１は、セキュア・コンテンツ・サーバ（ここでは、Secure Music Server：ＳＭＳで、以下、簡単にＳＭＳと呼ぶことがある）２を具備し、利用者が購入したコンテンツはＥＭＤインタフェース（Ｉ／Ｆ）部３を経由してＳＭＳ２に蓄積される。音楽コンテンツは、必要に応じてＥＭＤＩ／Ｆ部３で復号され、形式変換や再暗号化が施される。ＳＭＳ２が暗号化コンテンツを受け取ると、それを音楽データ格納部１０に格納し、音楽データ復号鍵をライセンス格納部９に格納する。ＳＭＳ２が再生機能を有していても良い。当該再生機能により、ＳＭＳ２が管理する音楽コンテンツをＰＣ上で再生する事ができる。

【００２１】ＳＭＳ２は、メディア（以下、簡単にＭＣ（memory card）と呼ぶことがある）１３に対してコンテンツデータを出力する機能を有している。ＭＣ１３を記録再生装置（以下、簡単にＰＤ（Portable Device）と呼ぶことがある）１２にセットし、ＭＣ１３に記録されたコンテンツを再生することができる。

【００２２】ＳＭＳ２からＭＣ１３へのコンテンツの記録はメディア（ＭＣ）インタフェース（Ｉ／Ｆ）部６を通じて直接行われるか、又はＰＤ１２を経由して行うことができる。

【００２３】デバイスＩＤ格納部４は、例えば、ＲＯＭで構成され、当該ＬＣＭの識別情報（デバイスＩＤ）が格納されている。

【００２４】ＭＣ１３は、そのメディア固有かつ書き換え不能の識別情報（ＭＩＤ）を有しており、ＭＣ１３に格納されるコンテンツは、ＭＣ１３に依存する暗号化鍵で暗号化されていてもよい。

【００２５】まず、チェックイン／チェックアウトについて、図１のＬＣＭ１に則して説明する。

【００２６】チェックアウトとは、ＬＭＳ１が「親」としてのコンテンツを格納しており、ＭＣ１３に、その複製を「子」コンテンツとしてコピーすることをいう。「子」コンテンツはＰＤ１２で自由に再生する事が可能であるが、「子」から「孫」コンテンツを作成する事は許されない。「親」が幾つ「子」を生むことができるかは、「親」の属性として定義される。また、チェックインとは、例えば、ＭＣ１３をＬＣＭ１に接続し、ＬＣＭ１が「子」コンテンツを消去（又は利用不能）する事で、ＬＣＭ１内の「親」コンテンツは「子」を１つ作る権利を回復することをいう。これを「親」にチェックインするともいう。

【００２７】このチェックイン／チェックアウトを単純に、従来からのＬＣＭ１で実現しようとすると、実際、次の様な「攻撃」が存在する。すなわち、ＭＣ１３に格納された「子」を別の記憶メディアに（ＭＩＤを除いて）退避しておき、ＭＣ１３の「子」を「親」にチェックインする。次いで、先に退避しておいた「子」を当該ＭＣ１３に書き戻す。既にチェックインは済んでいるので、ＬＣＭ１上の「親」は別のＭＣ１３に「子」をコピーして良い。この方法で、任意の個数だけ利用可能な「子」を作る事が可能である。

【００２８】上述の「攻撃」には、ＭＣ１３とＬＣＭ１とのデータ転送の際に認証を行う事により、対抗可能である。すなわち、ＭＣ１３は正当なＬＣＭ１以外からのデータ転送を受け付けず、ＬＣＭ１が正当なＭＣ１３以外からのデータ転送を受け付けないと仮定する。この場合、ＭＣ１３内の「子」を別の記録メディアに退避する事はできない。又、ＬＣＭ１に対して、偽って、チェックインすることもできない。従って、上述の「攻撃」は破綻する。

【００２９】ところが、実は、ＬＣＭ１とＭＣ１３との認証を前提としても、チェックイン／チェックアウトは実現できない。次の様な「攻撃」が存在するからである。すなわち、まず、ＬＣＭ１上の「親」が「子」を作っていない状態で、ＬＣＭ１のデータ（特に、ライセンス格納部９の情報）を別の記憶メディアにバックアップする。ＭＣ１３に「子」をコピーした後、バックアップしたＬＣＭ１のデータを復帰する。ＬＣＭ１の「親」は「子」を作る前の状態に戻るから、別のＭＣ１３に「子」を作成する事ができる。この様にして、任意の数の「子」を作成する事が可能となってしまう。

【００３０】そこで、このような攻撃にも対処できるチェックイン／チェックアウトを実現するために、ＭＣ１３内の記憶領域に、公開された手順では読み書きできない領域（秘匿領域）を設け、そこに相互認証に必要な情報やコンテンツ復号に必要な情報や、アクセス不可能であるデバイス（ＬＣＭ１、ＰＤ１２）の識別情報（デバイスＩＤ）のリスト（リボケーションリスト（ＲＶＣリスト））等を記録する（図２参照）。また、ＬＣＭ１の記憶領域（例えば、ＬＣＭ１がＰＣで構成されている場

合には、ハードディスク（ＨＤＤ）上に非公開の手順でしかアクセスできない領域（秘匿領域）を設け、後述するような宿帳を当該秘匿領域に格納する（図２参照）。さらに、ＰＤ１２の記憶領域上にも非公開の手順でしかアクセスできない領域（秘匿領域）を設け、そこにコンテンツ復号に必要な情報を記録するようにしてもよい（図２参照）。なお、ここでは、記憶領域中の秘匿領域以外の通常に手順にてアクセス可能な領域を公開領域と呼ぶ。

【００３１】図１に示すように、ＬＣＭ１では、秘匿領域には、宿帳格納部８が設けられ、ＳＭＳ２にてこの宿帳格納部８にアクセスするための秘匿された特定の手続が行われた後、秘匿領域からデータを読み取るための秘匿領域ドライバ７を具備している。

【００３２】図４（ｃ）に示すように、ＭＣ１３は、その識別情報ＭＩＤを格納するための外部からは書換不可能で、コピーも不可能なような構成になっている識別情報格納部（ＲＯＭ）１３ｂと、秘匿領域１３ｃと、公開領域（読み書き可能なＲＡＭ）１３ａと、秘匿領域１３ｃがアクセスされる際に認証部１３ｄにて認証を行って、正当な相手であると確認されたときに初めて秘匿領域１３ｃにアクセス可能なようにゲートを開くスイッチ（ＳＷ）１３ｅを具備する。

【００３３】なお、本実施形態で利用可能なＭＣ１３は、３種類あり、図４（ｃ）に示すような、識別情報ＭＩＤと秘匿領域とを両方兼ね備えているＭＣ１３の種別を「レベル２」と呼ぶ。秘匿領域は持たないが識別情報ＭＩＤは持つ図４（ｂ）に示すようなＭＣ１３の種別を「レベル１」と呼ぶ。秘匿領域も識別情報も持たない図４（ａ）に示すような公開領域だけのＭＣ１３の種別を「レベル０」と呼ぶことにする。これら種別は、例えば、識別情報ＭＩＤの有無でレベル０とそれ以外の種別とが判別でき、さらに、識別情報ＭＩＤの構成からレベル１とレベル２とを判別する。例えば、識別情報が連続した数値であるとき、所定値以上はレベル２であるとする。

【００３４】以下、特に断らない限り、レベル２のＭＣ１３の場合を例にとり説明する。

【００３５】このＭＣ１３は、ＬＣＭ１に接続されたＰＤ１２にセットして用いる場合とＬＣＭ１に直接セットして用いる場合とがある。

【００３６】図３は、ＰＤ１２の構成例を示したもので、ＭＣ１３は、メディアインタフェース（Ｉ／Ｆ部）１２ｆにセットされる。ＬＣＭ１がＰＤ１２を介してＭＣ１３に読み書きする場合は、ＰＤ１２内の秘匿領域アクセス部を経由してＭＣ１３の秘匿領域にアクセスする。メディアＩ／Ｆ部１２ｆには、ＭＣ１３の秘匿領域にアクセスするための秘匿領域アクセス部を具備している。ＰＤ１２内の秘匿領域は、フラッシュメモリ１２ｄに設けられていても良い。ＲＯＭ１２ｃには、ＭＣ１３、ＬＣＭ１との間で相互認証を行うためのプログラムや、秘匿領域へアクセスするための認証手続を記述したプログラムや、ＭＣ１３の種別を判別するためのプログラムも書き込まれていて、このプログラムに従って、ＣＰＵ１２ａの制御の下、ＭＣ１３との間の各種認証、種別判別等の処理を実行するようになっている。

【００３７】ＲＯＭ１２ｃには、ＰＤ１２の識別情報（デバイスＩＤ）が格納されていてもよい。また、例えば、フラッシュメモリ１２ｄに設けられた秘匿領域に秘匿デバイスＩＤ（ＳＰＤＩＤ）が予め格納されている。

【００３８】図５は、ＬＣＭ１のメディアＩ／Ｆ部６の構成を示したもので、ＭＣ１３との間で相互認証を行うための認証部６ｃと、ＭＣ１３の種別を判別するメディア判別部６ｂと、これら全体を制御するための制御部６ａとから構成されている。認証部６ｃは、ＭＣ１３の秘匿領域にアクセスするための秘匿領域アクセス部でもある。

【００３９】図２４は、図４（ｃ）に示したレベル２のＭＣ１３の構成をより具体的に示したものである。図２４に示すように、秘匿領域１０２は、例えば、１チップのメモリ素子（例えばＲＡＭ）上に構成され、ＲＡＭ領域とＲＯＭ領域とを有している。例えば、ＲＡＭ領域であるかＲＯＭ領域であるかは例えばＣＰＵ等から構成される制御部１０１によるアクセス制御の違いにより区別する。公開領域にはＲＯＭ領域１０３とＲＡＭ領域１０４とがそれぞれ別個のメモリ素子で構成されている。

【００４０】制御部１０１には、秘匿領域１０２へアクセスする際と公開領域１０３、１０４へアクセスする際とでそれぞれ別個のバスが接続されていて、制御部１０１は、いずれか一方のバスに切り替えて秘匿領域１０２、あるいは公開領域１０３、１０４へアクセスするようになっている。

【００４１】制御部１０１は、ＭＣ１３の各構成部の制御を司さどるとともに、ＬＣＭ１等がＭＣ１３の秘匿領域にアクセスする度に実行される認証処理（ＡＫＥ）も実行する。

【００４２】秘匿領域１０２中のＲＯＭ領域には、例えば、ＭＣ１３、ＬＣＭ１との間で相互認証を行うためのプログラムや、秘匿領域へアクセスするための認証処理（ＡＫＥ）を記述したプログラムや、秘匿メディアＩＤ（ＳＭＩＤ）等が予め格納されていてもよい。

【００４３】次に、ＬＣＭ１の秘匿領域に格納される宿帳について説明する。

【００４４】ＳＭＳ２にて保持する全ての音楽コンテンツは、そのそれぞれを識別するための識別情報であるコンテンツＩＤ（ＴＩＤ）と、予め定められた複製可能コンテンツ数、すなわち、子の残数とチェックアウトリストとをその属性情報として持つ。この属性情報を宿帳と呼ぶ。宿帳は、秘匿領域に設けられた宿帳格納部８に図７（ａ）に示すような形態で記録されている。

【００４５】図７（ａ）において、例えば、コンテンツＩＤ「ＴＩＤ１」なる子の残数は「２」で、そのチェックアウトリストはＬ１である。

【００４６】チェクアウトリストは、複製コンテンツ（子）を記録したＭＣ１３の識別情報のリストであって、例えば、図７（ａ）において、チェックアウトリストＬ１には「ｍ１」と「ｍ２」という識別情報を持つ２つのＭＣ１３にコンテンツＩＤ「ＴＩＤ１」なるコンテンツの子がチェックアウトされていることがわかる。

【００４７】以下、次に示す項目の順に説明する。

【００４８】（１）相互認証方法の概略

（２）レベル２のＭＣを用いた複製コンテンツのチェックイン／チェックアウト／再生

（３）レベル０のＭＣを用いた複製コンテンツのチェックイン／チェックアウト／再生

（１）相互認証方法の概略

前述したように、チェックイン／チェクアウトを安全に行うために、ＬＣＭ１、ＰＤ１２とＭＣ１３との間で（例えば、互いに同じアルゴリズムをもっているかの確認のための）相互認証を行う必要がある。一般に、相互認証処理には、相互認証を行う一方と他方とで共有する秘密の情報を持つ必要がある。従って、このような秘密情報を例えばＭＣ１３とＬＣＭ１およびＰＤ１２が持つことになる。情報セキュリティの観点から考えると、この秘密情報は、認証を行う度に毎回異なるものが生成されるといった動的なものであった方がよい。しかし、ＭＣ１３というメディア自体にそのような秘密情報を生成するための高度な機能を追加すると、メディアが高価になってしまう。メディアを広く一般大典に普及させるためには、できるだけ安価である方が望ましい。従って、メディア（ＭＣ１３）のコスト低減化を考えれば、秘密情報をＭＣ１３に予め記憶させておく方がよい。

【００４９】しかし、全てのメディア、あるいは一定数の複数のメディアで共通する秘密情報（以下、このような情報をグローバルシークレットな情報と呼ぶ）をそれぞれのメディアに予め記憶させた場合、ある１つのメディアからその秘密情報が何らかの方法により読まれてしまったとき、同じ秘密情報を記憶する他のメディアも不正に利用されてしまうという問題点があった。メディアにグローバルスシークレットな情報を持たせることは極めて危険である（図８（ａ）参照）。

【００５０】ある１つのメディアに記憶されている秘密情報が不当に読まれてしまっても、不正に使用できるのは、その秘密情報が読まれしまったメディアだけであれば問題がないわけであるから、秘密情報は、個々のメディアに固有のものであればよい。

【００５１】そこで、ここでは、個々のメディアにメディア毎にそれぞれ異なる相互認証のための秘密情報を記憶させておき、この情報を用いてＬＣＭ１あるいはＰＤ１２とＭＣ１３とが相互認証を行うことにより、低コストなメディアを用いた、よりセキュリティ性の高い安全な相互認証方法を提案する。すなわち、本実施形態で説明する相互認証方法は、図８（ｂ）に示すように、個々のメディア（レベル２のメディア）に相互認証（ＡＫＥ）のために必要な各メディア毎にそれぞれ異なる秘密情報（ここでは、秘匿メディアＩＤ（ＳＭＩＤ）で、これは、メディアＩＤを何らかの方法で取得した鍵情報ＫＭで予め暗号化されたもの）を（秘匿領域に）予め記憶させておき、ＬＣＭ１，ＰＤ１２には、そのメディアの識別情報（ＭＩＤ）を転送する。ＬＣＭ１あるいはＰＤ１２側では、ＭＩＤと、先に何らかの方法で取得した情報（ＫＭ）とを用いて相互認証のための情報（メディアのもつＳＭＩＤと同じもの）を所定のアルゴリズムを用いて生成して認証処理（ＡＫＥ）を行う。

【００５２】このように、ＭＣ１３にはそれぞれに固有の秘密情報（ＳＭＩＤ）を持たせておくだけで、ＬＣＭ１、ＰＤ１２がメディアから転送されてきた各メディア毎に固有の情報（ＭＩＤ）を基に秘密情報（ＳＭＩＤ）を生成することにより、メディアに負荷をかけずに安全な相互認証が行える。

【００５３】なお、以下の説明において、上記した相互認証処理をＡＫＥと呼ぶことにする。

【００５４】ＭＣ１３がＬＣＭ１のメディアＩ／Ｆ部６、あるいは、ＰＤ１２にセットされると、まず、メディアＩＦ部６とＭＣ１３との間、あるいは、ＰＤ１２とＭＣ１３との間で相互認証が行われてもよい（図９のステップＳ１）、そして、双方にて正当な（例えば、同じ規格のハードウエア構成である）相手であると判断されたとき（ステップＳ２）、メディアＩ／Ｆ部６あるいはＰＤ１２はＭＣ１３から読み取った識別情報ＭＩＤを基に、ＭＣ１３の種別を判別する（ステップＳ３）。そして、メディアＩ／Ｆ部６あるいはＰＤ１２は、その種別に応じたチェックイン／チェックアウト／再生処理を実行する（ステップＳ６）。

【００５５】なお、図９のステップＳ１における相互認証は、必ずしも図８（ｂ）に示したような相互認証である必要はない。

【００５６】また、ＭＣ１３にはレベル０からレベル２までの３種類があると説明したが、ここでは、レベル０とレベル２の２種類のＭＣ１３を対象として、図９以降の複製コンテンツのチェックイン／チェックアウト／再生処理動作について説明する。

【００５７】さらに、以下の説明では、省略しているが、ＬＣＭ１とＭＣ１３との間、ＬＣＭ１とＰＤ１２との間、ＰＤ１２とＭＣ１３との間で、それぞれの秘匿領域にアクセスする際には、一方と他方との間で相互認証を行い、双方の正当性が確認されたらそれぞれの秘匿領域へのゲートを開き、秘匿領域へのアクセスが終了したら秘匿領域へのアクセスを可能にしていたゲートを閉じる仕組みになっているものとする。例えば、ＬＣＭ１と

ＭＣ１３との間において、ＳＭＳ２は、ＭＣ１３の秘匿領域１３ｃにアクセスすべく、ＭＣ１３との間で相互認証を行い、双方の正当性が確認されてスイッチ１３ｅにより秘匿領域１３ｃへのゲートが開かれると、秘匿領域１３ｃ内に鍵情報等を書込み、それが終了すると秘匿領域１３ｃへのアクセスを可能にしていたゲートがスイッチ１３ｅにより閉じられる仕組みになっている。

【００５８】（２）　レベル２のＭＣを用いた複製コンテンツのチェックイン／チェックアウト／再生

図４（ｃ）に示したような構成のレベル２のＭＣ１３を用いたチェックイン／チェックアウト、再生処理動作について説明する。

【００５９】チェックアウトの指示がＬＣＭ１のユーザインタフェース（Ｉ／Ｆ）部１５を介して、あるいは、ＰＤ１２を介して（すなわち、ＭＣ１３をＬＣＭ１に接続されたＰＤ１２にセットして用いた場合）、ＳＭＳ２に対しなされた場合について、図１０を参照して説明する。

【００６０】ＳＭＳ２は、台帳のチェックアウト要求のあったコンテンツ（例えばコンテンツＩＤが「ＴＩＤ１」であるとする）の子の残数ｎを調べ、ｎ＞０のとき、デバイスＩＤ格納部４から当該ＬＣＭ１のデバイスＩＤ（ＬＣＭＩＤ）を読み出し、それをＭＣ１３へ転送する（ステップＳ１０１）。

【００６１】ＭＣ１３では、転送されてきたデバイスＩＤがＲＶＣリストに登録されていないかチェックし（ステップＳ１０２）、登録されていないとき秘匿領域１３ｃにアクセスしてマスターキーＫＭを読み出して、ＬＣＭ１へ転送する（ステップＳ１０３）。ＭＣ１３は、さらに、識別情報格納部１３ｂから、その識別情報（ＭＩＤ）を読み出して同じくＬＣＭ１へ転送する（ステップＳ１０４）。

【００６２】ＬＣＭ１では、ＭＣ１３から転送されてきたメディアＩＤ（ＭＩＤ）をマスターキーＫＭで暗号化して、相互認証処理（ＡＫＥ）に必要な情報（ＫＭ［ＭＩＤ］）を生成する（ステップＳ１０５）。

【００６３】ＬＣＭ１では、この生成された情報ＫＭ［ＭＩＤ］を用いて相互認証処理（ＡＫＥ）を実行し、一方、ＭＣ１３でも秘匿メディアＩＤ（ＳＭＩＤ）を用いて相互認証処理（ＡＫＥ）を実行する（ステップＳ１０６）。この相互認証処理（ＡＫＥ）では、ＬＣＭ１とＭＣ１３とが同じ関数ｇ（ｘ，ｙ）、Ｈ（ｘ，ｙ）を共有していて、ＬＣＭ１で生成された情報ＫＭ［ＭＩＤ］が当該ＭＣ１３の秘匿メディアＩＤ（ＳＭＩＤ）と同じであるならば、相互認証処理（ＡＫＥ）により互いに一方が他方を正当であると確認できるようになっている。

【００６４】ここで、図２２を参照して、ステップＳ１０６の相互認証処理（ＡＫＥ）の処理動作について説明する。

【００６５】ＬＣＭ１は、乱数Ｒ１を発生し（ステップＳ３０１）して、それをＭＣ１３に転送するとともに、２つの変数ｘ、ｙを有する関数ｇ（ｘ，ｙ）の一方の変数に代入する。また、図１０のステップＳ１０５で生成された情報ＫＭ［ＭＩＤ］を関数ｇ（ｘ，ｙ）の他方の変数に代入して、関数ｇの値を求める（ステップＳ３０２）。

【００６６】一方、ＭＣ１３でも、ＬＣＭ１から転送されてきた乱数Ｒ１を関数ｇ（ｘ，ｙ）の一方の変数に代入し、自身の秘匿メディアＩＤ（ＳＭＩＤ）を他方の変数に代入して、求めた関数ｇの値をＬＣＭ１へ転送する（ステップＳ３０３）。

【００６７】ＬＣＭ１では、ＭＣ１３から転送されてきた関数ｇの値と、ＬＣＭ１側で求めた関数ｇの値とを比較し、一致していたら後続の処理を実行する。また、不一致であれば、この時点で、ＬＣＭ１側でのＡＫＥの処理を中止する（ステップＳ３０４）。

【００６８】次に、ＭＣ１３では、乱数Ｒ２を発生し（ステップＳ３０５）して、それをＬＣＭ１に転送するとともに、２つの変数を有する関数ｇ（ｘ，ｙ）の一方の変数に代入する。また、当該ＭＣ１３の秘匿メディアＩＤ（ＳＭＩＤ）を関数ｇ（ｘ，ｙ）の他方の変数に代入して、関数ｇの値を求める（ステップＳ３０６）。

【００６９】一方、ＬＣＭ１でも、ＭＣ１３から転送されてきた乱数Ｒ２を関数ｇ（ｘ，ｙ）の一方の変数に代入し、また、図１０のステップＳ１０５で生成された情報ＫＭ［ＭＩＤ］を関数ｇ（ｘ，ｙ）の他方の変数に代入して、関数ｇの値を求めたら、それをＭＣ１３へ転送する（ステップＳ３０７）。

【００７０】ＭＣ１３では、ＬＣＭ１から転送されてきた関数ｇの値と、ＭＣ１３側で求めた関数ｇの値とを比較し、一致していたら後続の処理を実行する。また、不一致であれば、この時点で、ＭＣ１３側でのＡＫＥの処理を中止する（ステップＳ３０８）。

【００７１】ＭＣ１３では、ステップＳ３０８で、関数ｇの値が一致していたら、２つの変数を有する関数Ｈ（ｘ，ｙ）の一方の変数に乱数Ｒ２、他方の変数に当該ＭＣ１３の秘匿メディアＩＤ（ＳＭＩＤ）を代入して鍵情報ＫＴを生成する（ステップＳ３０９）。

【００７２】一方、ＬＣＭ１でも、ステップＳ３０４で関数ｇの値が一致していたら、ＭＣ１３から転送されてきた乱数Ｒ２を関数Ｈ（ｘ，ｙ）の一方の変数に代入するとともに、図１０のステップＳ１０５で生成された情報ＫＭ［ＭＩＤ］を他方の変数に代入して鍵情報ＫＴを生成する（ステップＳ３１０）。

【００７３】なお、ステップＳ３０４、ステップＳ３０８のそれぞれで関数ｇの値が一致したことによりＬＣＭ１とＭＣ１３のそれぞれで同じ関数Ｈ（ｘ，ｙ）を用いて生成される鍵情報ＫＴは同じものである。ＬＣＭ１とＭＣ１３のそれぞれでは、以降、この鍵情報ＫＴを用いてコンテンツ復号鍵Ｋｃの受け渡しを行うようになって

いる。

【0074】また、相互認証処理（AKE）で生成される鍵情報KTは、毎回異なるものである方が情報セキュリティ上望ましい。ここでは、鍵情報KTを生成する関数Hに代入される2つの変数のうちの一方には、毎回新たに生成される乱数R2が代入されるので、毎回個となる鍵情報KTが生成される。

【0075】図10の説明に戻り、ステップS106において、LCM1とMC13との間で相互に認証されたときは、MC13では、生成した鍵情報KT（ここでは、KT1とする）を秘匿領域に格納する（ステップS107）。また、LCM1では、暗号化コンテンツを復号するための復号鍵（コンテンツ復号鍵）Kcをステップ S106で生成された鍵情報KT1で暗号化して（KT1［Kc］）MC13へ転送し（ステップS108～ステップS109）、コンテンツ情報CをKcで暗号化して（Kc［C］）MC13へ転送する（ステップS110～ステップS111）。

【0076】最後に、SMS2は、図7（b）に示すように、前回のチェックアウト要求のあったコンテンツID「TID1」のコンテンツの子の残数nから「1」減算し、チェックアウトリストL1に、当該MC13の識別情報「m0」を追加する。

【0077】MC13は、転送されてきた暗号化されたコンテンツ復号鍵KT1［Kc］、暗号化コンテンツKc［C］を公開領域13aに格納する。

【0078】以上の処理が終了したときのMC13の記憶内容を図6に示す。

【0079】次に、再生の指示がLCM1のユーザインタフェース（I／F）部15を介してSMS2に、あるいは、PD12に対しなされた場合について、図11を参照して説明する。

【0080】まず、PD12あるいはLCM1は、自身のデバイスIDをMC13へ転送する（ステップS121）。

【0081】LCM1が図3に示すようなPD2のコンテンツの再生機能部（復調部12g、デコーダ12h、D／A変換部121等）を持っているのであれば、MC13をPD12で再生する場合もLCM1で再生する場合も同様であるので、以下、PD12で再生する場合を例にとり説明する。

【0082】MC13では、転送されてきたデバイスIDがRVCリストに登録されていないかチェックし（ステップS122）、登録されていないとき秘匿領域13cにアクセスしてマスターキーKMを読み出して、PD12へ転送する（ステップS123）。MC13は、さらに、識別情報格納部13bから、その識別情報（MID）を読み出して同じくPD12へ転送する（ステップS124）。

【0083】PD12では、MC13から転送されてきたメディアID（MID）をマスターキーKMで暗号化して、相互認証処理（AKE）に必要な情報（KM［MID］）を生成する（ステップS125）。

【0084】PD12では、この生成された情報KM［MID］を用いて相互認証処理（AKE）を実行し、一方、MC13でも秘匿メディアID（SMID）を用いて相互認証処理（AKE）を実行する（ステップS126）。ステップS126の相互認証処理（AKE）は、図22と同様であるので説明は省略する。

【0085】PD12とMC13との間で相互に認証されたときは、MC13では、生成した鍵情報KT（ここでは、KT2とする）を用いて秘匿領域13cに格納されていた鍵情報KT1を暗号化して（KT2［KT1］）、PD12へ転送する（ステップS127～ステップS128）。一方、PD12では、ステップS126で生成された鍵情報KT2を用いてMC13から転送されてきたKT2［KT1］を復号することができる（ステップS128）。

【0086】MC13からは暗号化されたコンテンツ復号鍵KT1［Kc］、暗号化コンテンツKc［C］を公開領域13aから読み出してPD12へ転送する（ステップS129、ステップS131）。

【0087】PD12は、鍵情報KT1の復号に成功していれば、それを用いて暗号化されたコンテンツ復号鍵KT1［Kc］を復号してコンテンツ復号鍵Kcが得られるので（ステップS130）、このコンテンツ復号鍵Kcを用いて暗号化コンテンツKc［C］を復号して、コンテンツCを得る（ステップS132）。そして、PD12では、コンテンツCをデコーダ12hでデコードして、D／A変換部121でデジタル信号からアナログ信号に変換し、MC13に記録されていた複製コンテンツ（例えば音楽）を再生することができる。

【0088】次に、チェックインの指示がLCM1のユーザインタフェース（I／F）部15を介して、あるいは、PD12を介して（すなわち、MC13をLCM1に接続されたPD12にセットして用いた場合）、SMS2になされた場合について、図12を参照して説明する。

【0089】図12に示すチェックイン時の処理動作は、MC13に記録した鍵情報（あるいは鍵情報と暗号化コンテンツ情報）を消去（乱数で上書き消去）する際と、消去されたことの確認を行う際との合計2回、相互認証処理（AKE）を行うものである。

【0090】SMS2は、デバイスID格納部4から当該LCM1のデバイスID（LCMID）を読み出し、それをMC13へ転送する（ステップS141）。

【0091】MC13では、転送されてきたデバイスIDがRVCリストに登録されていないかチェックし（ステップS142）、登録されていないとき秘匿領域13cにアクセスしてマスターキーKMを読み出して、LC

ＭＩへ転送する（ステップＳ１４３）。ＭＣ１３は、さらに、識別情報格納部１３ｂから、その識別情報（ＭＩＤ）を読み出して同じくＬＣＭ１へ転送する（ステップＳ１４４）。

【００９２】ＬＣＭ１では、ＭＣ１３から転送されてきたメディアＩＤ（ＭＩＤ）をマスターキーＫＭで暗号化して、相互認証処理（ＡＫＥ）に必要な情報（ＫＭ［ＭＩＤ］）を生成する（ステップＳ１４５）。

【００９３】ＬＣＭ１では、この生成された情報ＫＭ［ＭＩＤ］を用いて第１の相互認証処理（ＡＫＥ＃１）を実行し、一方、ＭＣ１３でも秘匿メディアＩＤ（ＳＭＩＤ）を用いて第１の相互認証処理（ＡＫＥ＃１）を実行する（ステップＳ１４６）。

【００９４】ステップＳ１４６の相互認証処理（ＡＫＥ＃１）は、図２２と同様であるので説明は省略する。

【００９５】ステップＳ１４６において、ＬＣＭ１とＭＣ１３との間で相互に認証されたときは、ＬＣＭ１では、ＭＣ１３の秘匿領域（ＲＡＭ領域）１３ｃに格納されている鍵情報ＫＴ１に上書きするための乱数ｒ１を従来からある乱数発生器を用いて発生して、それとＭＣ１３への上書き指示情報とをステップＳ１４６で生成した鍵情報ＫＴ（ここではＫＴ３とする）で暗号化して（ＫＴ３［上書指示＋ｒ１］）ＭＣ１３へ転送する（ステップＳ５０１）。なお、上書指示には、鍵情報ＫＴ１の書き込まれているアドレスが含まれていてもよい。

【００９６】ＭＣ１３では、ＬＣＭ１から転送されてきたＫＴ３［上書指示＋ｒ１］をステップＳ１４６で生成した鍵情報ＫＴ３で復号し、乱数ｒ１を得る（ステップＳ５０２）。この乱数ｒ１で、ＭＣ１３の秘匿領域（ＲＡＭ領域）１３ｃに格納されている鍵情報ＫＴ１を上書きすることで消去する（ステップＳ５０３）。なお、鍵情報ＫＴ１の他に、さらにコンテンツ復号鍵Ｋｃを鍵情報ＫＴ１で暗号化したもの（ＫＴ１［Ｋｃ］）や暗号化コンテンツ情報Ｋｃ［Ｃ］も乱数ｒ１で上書きすることで消去してもよい。

【００９７】次に、鍵情報ＫＴ１（あるいは、鍵情報ＫＴ１と暗号化コンテンツ情報等）が乱数ｒ１にて確実に消去されたか否かの確認のための処理を実行する。すなわち、ＬＣＭ１では、ステップＳ１４５で生成された情報ＫＭ［ＭＩＤ］を用いて第２の相互認証処理（ＡＫＥ＃２）を実行し、一方、ＭＣ１３でも秘匿メディアＩＤ（ＳＭＩＤ）を用いて第２の相互認証処理（ＡＫＥ＃２）を実行する（ステップＳ５０４）。

【００９８】ステップＳ５０４の第２の相互認証処理（ＡＫＥ＃２）は、図２２と同様であるので説明は省略する。

【００９９】ステップＳ５０４において、ＬＣＭ１とＭＣ１３との間で相互に認証されたときは、ＭＣ１３は、鍵情報ＫＴ１（あるいは、鍵情報ＫＴ１と暗号化コンテンツ情報等）が格納されていたアドレスからデータ（正常に上書きされていれば、乱数ｒ１）を読み取って、それをステップＳ５０４で生成された鍵情報ＫＴ（ここではＫＴ４とする）で暗号化して（ＫＴ４［ｒ１］）ＬＣＭ１へ転送する（ステップＳ５０５）。

【０１００】ＬＣＭ１では、ＭＣ１３から転送されてきたＫＴ４［ｒ１］をステップＳ５０４で生成した鍵情報ＫＴ４で復号し（ステップＳ５０６）、その際得られたデータとステップＳ５０１で発生した乱数ｒ１とを比較し、一致していれば、ＭＣ１３において、鍵情報ＫＴ１（あるいは、鍵情報ＫＴ１と暗号化コンテンツ情報等）が乱数ｒ１にて消去されたと判断し、処理を終了する（ステップＳ５０７）。不一致のときはＬＣＭ１は異常を通知する等の処置を講ずるのが望ましい。

【０１０１】最後に、図７（ｃ）に示すように、前回のチェックイン要求のあったコンテンツＩＤ「ＴＩＤ１」のコンテンツの予の残数ｎに「１」加算し、チェックアウトリストＬ１から、当該ＭＣ１３の識別情報ｍ０を削除する。

【０１０２】次に、図１２とは異なる他のチェックイン時の処理動作について、図１３を参照して説明する。なお、図１２と同一部分には同一符号を付し、異なる部分について説明する。すなわち、図１３に示すチェックイン時の処理動作は、ＭＣ１３に記録した鍵情報（あるいは鍵情報と暗号化コンテンツ情報）を消去するための指示情報（例えば、これからチェックインを行う旨の指示情報）の転送の際と、実際に消去するためのコマンド発生のトリガとしての合計２回、相互認証処理（ＡＫＥ）を行う点に特徴があり、ステップＳ１４６のＡＫＥ＃１までの処理動作は図１２と同様である。

【０１０３】ステップＳ１４６において、ＬＣＭ１とＭＣ１３との間で相互に認証されたときは、ＬＣＭ１では、これからチェックインを行う旨の指示情報をステップＳ１４６で生成した鍵情報ＫＴ（ここではＫＴ３とする）で暗号化して（ＫＴ３［チェックイン指示］）ＭＣ１３へ転送する（ステップＳ５５１）。なお、チェックイン指示には、鍵情報ＫＴ１の書き込まれているアドレスが含まれていてもよい。

【０１０４】ＭＣ１３では、ＬＣＭ１から転送されてきたＫＴ３［チェックイン指示］をステップＳ１４６で生成した鍵情報ＫＴ３で復号し、チェックイン指示情報を得る（ステップＳ５５２）。

【０１０５】次に、実際に消去するためのコマンド発生のトリガとしての第２の相互認証処理（ＡＫＥ＃２）を実行する（ステップＳ５５３）。ここでのＡＫＥ＃２は、図２３に示すように、図２２のステップＳ３０８と同様にして、関数ｇの値が一致していたか否かをチェックしたら、その結果を出力するのみである。

【０１０６】ＭＣ１３では、関数ｇの値が一致していて、かつ、先にチェックイン指示情報を得ていたときは、鍵情報ＫＴ１（あるいは、鍵情報ＫＴ１と暗号化コ

ンテンツ情報等）を消去する（ステップＳ５５４～ステップＳ５５５）。例えば、ＭＣ１３のファイル管理領域を書き換えることにより鍵情報ＫＴ１等を消去するようにしてもよい。

【０１０７】最後に、図７（ｃ）に示すように、宿舗のチェックイン要求のあったコンテンツＩＤ「ＴＩＤ１」のコンテンツの子の残数ｎに「１」加算し、チェックアウトリストＬ１から、当該ＭＣ１３の識別情報ｍ０を削除する。

【０１０８】次に、図１０とは異なる他のチェックアウト時の処理動作について、図１４を参照して説明する。なお、図１０と同一部分には同一符号を付し、異なる部分について説明する。すなわち、図１４では、ＭＣ１３へ転送すべきコンテンツ復号鍵Ｋｃに対する処理に特徴がある。

【０１０９】図１４において、ＬＣＭ１では、コンテンツ復号鍵Ｋｃに対し、まず、ステップＳ１０５で生成されたＫｍ［ＭＩＤ］（以下、これをｗと表す）を用いて暗号化を施す（ステップＳ１６２）。そして、ｗで暗号化されたコンテンツ復号鍵Ｋｃ（ｗ［Ｋｃ］）をステップＳ１０６の相互認証処理（ＡＫＥ）にて生成した鍵情報ＫＴ１を用いてさらに暗号化を行ってから（ＫＴ１［ｗ［Ｋｃ］］）、ＭＣ１３へ転送する（ステップＳ１６３）。

【０１１０】ＭＣ１３では、ステップＳ１０６の相互認証処理（ＡＫＥ）にて生成した鍵情報ＫＴ１を用いて、転送されてきたＫＴ１［ｗ［Ｋｃ］］を復号してｗ［Ｋｃ］を得、これを秘匿領域１３ｃへ格納する（ステップＳ１６４）。

【０１１１】コンテンツ情報Ｃは、図１０の場合と同様に、Ｋｃで暗号化してから（ステップＳ１６５）、ＭＣ１３へ転送される（ステップＳ１６６）。

【０１１２】図１４に示したようなチェックアウト処理動作に対応する再生処理動作について、図１５を参照して説明する。なお、図１１と同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、図１５において、ＭＣ１３は、秘匿領域１３ｃに格納されている暗号化コンテンツ復号鍵ｗ［Ｋｃ］をステップＳ１２６の相互認証処理（ＡＫＥ）で生成された鍵情報ＫＴ２で暗号化してから（ＫＴ２［ｗ［Ｋｃ］］）ＬＣＭ１あるいはＰＤ１２へ転送する。（ステップＳ１７２）。ＬＣＭ１あるいはＰＤ１２では、同じくステップＳ１２６で生成された鍵情報ＫＴ２でＭＣ１３から転送されてきたＫＴ２［ｗ［Ｋｃ］］を復号して（ステップＳ１７３）、その結果得られたｗ［Ｋｃ］をステップＳ１２３で生成されたｗ＝ＫＭ［ＭＩＤ］を用いて復号して、コンテンツ復号鍵Ｋｃを得る（ステップＳ１７４）。このコンテンツ復号鍵Ｋｃを用いて暗号化コンテンツＫｃ［Ｃ］を復号して、コンテンツＣを得る（ステップＳ１７５）。そして、ＬＣＭ１あるいはＰＤ１２では、コンテンツＣをデコーダ１２ｈでデコードして、Ｄ／Ａ変換部１２１でデジタル信号からアナログ信号に変換し、ＭＣ１３に記録されていた複製コンテンツ（例えば音楽）を再生することができる。

【０１１３】図１４に示したようなチェックアウト処理動作に対応するチェックイン処理動作は、図１２、図１３の説明とほぼ同様で、異なるのは、図１２のステップＳ５０３、図１３のステップＳ５５５でＭＣ１３の秘匿領域１３ｃから消去されるのは、鍵情報ＫＴ１ではなく、ｗ＝ＫＭ［ＭＩＤ］で暗号化されたコンテンツ復号鍵ｗ［Ｋｃ］であるという点である。

【０１１４】（３）レベル０のＭＣを用いた複製コンテンツのチェックイン／チェックアウト／再生

次に、図４（ａ）に示したような構成のレベル０のＭＣ１３を用いたチェックイン／チェックアウト、再生処理動作について説明する。

【０１１５】この場合、ＭＣ１３は、ＰＤ１２にセットされ、このＰＤ１２を介してＬＣＭ１との間でチェックアウト処理が実行される。基本的な動作は、ＭＣ１３がレベル２の場合と同様であるが、レベル０の場合、秘匿領域、メディアＩＤを有していないので、ＰＤ１２がＬＣＭ１に対する処理をレベル０のＭＣ１３に代行して図１０に示したような処理を実行することとなる。そのため、ＰＤ１２の秘匿領域には、マスターキーＫＭ、秘匿デバイスキーＳＰＤＩＤ、リボケーションリスト（ＲＶＣリスト）を予め記憶しておくものとする。なお、マスターキーＫＭは必ずしもメディアＭＣ１３に記憶しておくマスターキーＫＭとその機能は同じであるが、そのデータ自体は同じものである必要はない。

【０１１６】まず、図９のステップＳ３において、ＭＣ１３の種別がレベル０であると判定される。

【０１１７】チェックアウトの指示がＬＣＭ１のユーザインタフェース（Ｉ／Ｆ）部１５を介して、あるいは、ＰＤ１２を介してＳＭＳ２に対しなされた場合について、図１６を参照して説明する。

【０１１８】ＳＭＳ２は、宿舗のチェックアウト要求のあったコンテンツ（例えばコンテンツＩＤが「ＴＩＤ１」であるとする）の子の残数ｎを調べ、ｎ＞０のとき、デバイスＩＤ格納部４から当該ＬＣＭ１のデバイスＩＤ（ＬＣＭＩＤ）を読み出し、それをＰＤ１２へ転送する（ステップＳ２０１）。

【０１１９】ＰＤ１２では、転送されてきたデバイスＩＤがＲＶＣリストに登録されていないかチェックし（ステップＳ２０２）、登録されていないときＰＤ１２の秘匿領域にアクセスしてマスターキーＫＭを読み出して、ＬＣＭ１へ転送する（ステップＳ２０３）。ＰＤ１２は、さらに、例えばＲＯＭ１２ｃからその識別情報..すなわち、デバイスＩＤ（ＰＤＩＤ）を読み出して、同じくＬＣＭ１へ転送する（ステップＳ２０４）。

【０１２０】ＬＣＭ１では、ＰＤ１２から転送されてき

19

たデバイスＩＤ（ＰＤＩＤ）をマスターキーＫＭで暗号化して、相互認証処理（ＡＫＥ）に必要な情報（ＫＭ［ＰＤＩＤ］）を生成する（ステップＳ２０５）。

【０１２１】ＬＣＭ１では、この生成された情報ＫＭ［ＰＤＩＤ］を用いて相互認証処理（ＡＫＥ）を実行し、一方、ＰＤ１２でも秘匿デバイスＩＤ（ＳＰＤＩＤ）を用いて相互認証処理（ＡＫＥ）を実行する（ステップＳ２０６）。ステップＳ２０６の相互認証処理（ＡＫＥ）は、図２２と同様であるので説明は省略する。

【０１２２】ＬＣＭ１とＰＤ１２との間で相互に認証されたとき、ＰＤ１２では、生成した鍵情報ＫＴ（ここでは、ＫＴ１とする）を秘匿領域に格納する（ステップＳ２０７）。ＬＣＭ１では、暗号化コンテンツを復号するための復号鍵（コンテンツ復号鍵）Ｋｃをステップ２０６で生成された鍵情報ＫＴ１で暗号化して（ＫＴ１［Ｋｃ］）、ＰＤ１２を経由してＭＣ１３へ転送し（ステップＳ２０８～ステップＳ２０９）、また、コンテンツ情報ＣをＫｃで暗号化して（Ｋｃ［Ｃ］）、ＰＤ１２を経由してＭＣ１３へ転送する（ステップＳ２１０～ステップＳ２１１）。

【０１２３】最後に、ＳＭＳ２は、図７（ｂ）に示すように、宿泊のチェックアウト要求のあったコンテンツＩＤ「ＴＩＤ１」のコンテンツの子の残数ｎから「１」減算し、チェックアウトリストＬ１に、当該ＰＤ１２の識別情報ＰＤＩＤを追加する。

【０１２４】ＭＣ１３は、転送されてきた暗号化されたコンテンツ復号鍵ＫＴ１［Ｋｃ］、暗号化コンテンツＫｃ［Ｃ］を公開領域１３ａに格納する。

【０１２５】次に、再生の指示がＰＤ１２に対しなされた場合のＰＤ１２とＭＣ１３との間の処理動作について、図１７を参照して説明する。

【０１２６】まず、ＭＣ１３は、公開領域に記録されている暗号化されたコンテンツ復号鍵ＫＴ１［Ｋｃ］をＰＤ１２へ転送する（ステップＳ２２１）。ＰＤ１２が当該ＭＣ１３に対し当該再生対象のコンテンツ情報をチェックアウトした際に用いたものであるならば、その秘匿領域に暗号化されたコンテンツ復号鍵を復号するための鍵情報ＫＴ１を記憶している（図１６のステップＳ２０７参照）。従って、そのような正当なＰＤ１２であるならば、秘匿領域から読み出した鍵情報ＫＴ１を用いて、ＭＣ１３から転送されてきたＫＴ１［Ｋｃ］を復号して、コンテンツ復号鍵Ｋｃを得ることができる（ステップＳ２２２）。さらに、このコンテンツ復号鍵Ｋｃを用いて、ＭＣ１３から転送されてきた暗号化コンテンツ情報Ｋｃ［Ｃ］を復号してコンテンツＣを得ることができる（ステップＳ２２３～ステップＳ２２４）。そして、ＰＤ１２では、コンテンツＣをデコーダ１２ｈでデコードして、Ｄ／Ａ変換部１２ｉでデジタル信号からアナログ信号に変換し、ＭＣ１３に記録されていた複製コンテンツ（例えば音楽）を再生することができる。

20

【０１２７】次に、チェックインの指示がＰＤ１２を介して（すなわち、ＭＣ１３をＬＣＭ１に接続されたＰＤ１２にセットして用いて）、ＳＭＳ２になされた場合について、図１８を参照して説明する。この場合もチェックアウトの場合と同様、ＰＤ１２がＬＣＭ１に対する処理をレベル０のＭＣ１３に代行して図１２に示したような処理を実行することとなる。

【０１２８】ＳＭＳ２は、デバイスＩＤ格納部４から当該ＬＣＭ１のデバイスＩＤ（ＬＣＭＩＤ）を読み出し、それをＰＤ１２へ転送する（ステップＳ２３１）。

【０１２９】ＰＤ１２では、転送されてきたデバイスＩＤがＲＶＣリストに登録されていないかチェックし（ステップＳ２３２）、登録されていないとき秘匿領域にアクセスしてマスターキーＫＭを読み出して、ＬＣＭ１へ転送する（ステップＳ２３３）。ＰＤ１２は、さらに、その識別情報（ＰＤＩＤ）を読み出して同じくＬＣＭ１へ転送する（ステップＳ２３４）。

【０１３０】ＬＣＭ１では、ＰＤ１２から転送されてきたデバイスＩＤ（ＰＤＩＤ）をマスターキーＫＭで暗号化して、相互認証処理（ＡＫＥ）に必要な情報（ＫＭ［ＰＤＩＤ］）を生成する（ステップＳ２３５）。

【０１３１】ＬＣＭ１では、この生成された情報ＫＭ［ＰＤＩＤ］を用いて第１の相互認証処理（ＡＫＥ＃１）を実行し、一方、ＰＤ１２でも秘匿デバイスＩＤ（ＳＰＤＩＤ）を用いて第１の相互認証処理（ＡＫＥ＃１）を実行する（ステップＳ２３６）。

【０１３２】チェックインの際のステップＳ２３６の第１の相互認証処理（ＡＫＥ＃１）動作は、図２２において、ＫＭ［ＭＩＤ］をＫＭ［ＰＤＩＤ］に置き換え、秘匿メディアＩＤ（ＳＭＩＤ）が秘匿デバイスＩＤ（ＳＰＤＩＤ）に置き換えれば同様であるので、説明は省略する。

【０１３３】ステップＳ２３６において、ＬＣＭ１とＰＤ１２との間で相互に認証されたときは、ＬＣＭ１では、ＰＤ１２の秘匿領域（ＲＡＭ領域）に格納されている鍵情報ＫＴ１に上書きするための乱数ｒ１を従来からある乱数発生器を用いて発生して、それとＭＣ１３への上書き指示情報とをステップＳ２３６で生成した鍵情報ＫＴ（ここではＫＴ３とする）で暗号化して（ＫＴ３［上書指示＋ｒ１］）ＰＤ１２へ転送する（ステップＳ６０１）。なお、上書指示には、鍵情報ＫＴ１の書き込まれているアドレスが含まれていてもよい。

【０１３４】ＰＤ１２では、ＬＣＭ１から転送されてきたＫＴ３［上書指示＋ｒ１］をステップＳ２３６で生成した鍵情報ＫＴ３で復号し、乱数ｒ１を得る（ステップＳ６０２）。この乱数ｒ１で、ＰＤ１２の秘匿領域に格納されている鍵情報ＫＴ１を上書きすることで消去する（ステップＳ６０３）。

【０１３５】次に、鍵情報ＫＴ１が乱数ｒ１にて確実に消去されたか否かの確認のための処理を実行する。すな

わち、ＬＣＭ１では、ステップＳ２３５で生成された情報KM［ＰＤＩＤ］を用いて第２の相互認証処理（ＡＫＥ＃２）を実行し、一方、ＰＤ１２でも秘匿デバイスＩＤ（ＳＰＤＩＤ）を用いて第２の相互認証処理（ＡＫＥ＃２）を実行する（ステップＳ６０４）。

【０１３６】ステップＳ６０４の第２の相互認証処理（ＡＫＥ＃２）は、ステップＳ２３６のＡＫＥ＃１と同様であるので説明は省略する。

【０１３７】ステップＳ６０４において、ＬＣＭ１とＰＤ１２との間で相互に認証されたときは、ＰＤ１２は、鍵情報ＫＴ１が格納されていたアドレスからデータ（正常に上書きされていれば、乱数ｒ１）を読み取って、それをステップＳ６０４で生成された鍵情報ＫＴ（ここではＫＴ４とする）で暗号化して（ＫＴ４［ｒ１］）ＬＣＭ１へ転送する（ステップＳ６０５）。

【０１３８】ＬＣＭ１では、ＰＤ１２から転送されてきたＫＴ４［ｒ１］をステップＳ６０４で生成した鍵情報ＫＴ４復号し（ステップＳ６０６）、その際得られたデータとステップＳ６０１で発生した乱数ｒ１とを比較し、一致していれば、ＰＤ１２において、鍵情報ＫＴ１（あるいは、鍵情報ＫＴ１と暗号化コンテンツ情報等）が乱数ｒ１にて消去されたと判断し、処理を終了する（ステップＳ６０７）。不一致のときはＬＣＭ１は異常を通知する等の処置を講ずるのが望ましい。

【０１３９】最後に、図７（ｃ）に示すように、宿帳のチェックイン要求のあったコンテンツＩＤ「ＴＩＤ１」のコンテンツの子の残数ｎに「１」加算し、チェックアウトリストＬ１から、当該ＰＤ１２の識別情報を削除する。

【０１４０】次に、図１８とは異なる他のチェックイン時の処理動作について、図１９を参照して説明する。なお、図１８と同一部分には同一符号を付し、異なる部分について説明する。すなわち、図１９に示すチェックイン時の処理動作は、ＰＤ１２に記録した鍵情報を消去するための指示情報（例えば、これからチェックインを行う旨の指示情報）の転送の際と、実際に消去するためのコマンド発生のトリガとしての合計２回、相互認証処理（ＡＫＥ）を行う点に特徴があり、ステップＳ２３６のＡＫＥ＃１までの処理動作は図１８と同様である。

【０１４１】ステップＳ２３６において、ＬＣＭ１とＰＤ１２との間で相互に認証されたときは、ＬＣＭ１では、これからチェックインを行う旨の指示情報をステップＳ２３６で生成した鍵情報ＫＴ（ここではＫＴ３とする）で暗号化して（ＫＴ３［チェックイン指示］）ＰＤ１２へ転送する（ステップＳ６５１）。なお、チェックイン指示には、鍵情報ＫＴ１の書き込まれているアドレスが含まれていてもよい。

【０１４２】ＰＤ１２では、ＬＣＭ１から転送されてきたＫＴ３［チェックイン指示］をステップＳ２３６で生成した鍵情報ＫＴ３で復号し、チェックイン指示情報を得る（ステップＳ６５２）。

【０１４３】次に、実際に消去するためのコマンド発生のトリガとしての第２の相互認証処理（ＡＫＥ＃２）を実行する（ステップＳ６５３）。ここでのＡＫＥ＃２は、図２３に示すように、図２２のステップＳ３０８と同様にして、関数ｇの値が一致していたか否かをチェックしたら、その結果を出力するのみである。

【０１４４】ＰＤ１２では、関数ｇの値が一致していて、かつ、先にチェックイン指示情報を得ていたときは、鍵情報ＫＴ１を消去する（ステップＳ６５４～ステップＳ６５５）。例えば、ＰＤ１２のファイル管理領域を書き換えることにより鍵情報ＫＴ１等を消去するようにしてもよい。

【０１４５】最後に、図７（ｃ）に示すように、宿帳のチェックイン要求のあったコンテンツＩＤ「ＴＩＤ１」のコンテンツの子の残数ｎに「１」加算し、チェックアウトリストＬ１から、当該ＰＤ１２の識別情報を削除する。

【０１４６】次に、図１６とは異なる他のチェックアウト時の処理動作について、図２０を参照して説明する。なお、図１６と同一部分には同一符号を付し、異なる部分について説明する。すなわち、図２０では、図１４の場合と同様に、ＰＤ１２へ転送すべきコンテンツ復号鍵Ｋｃに対する処理に特徴がある。

【０１４７】図２０において、ＬＣＭ１では、コンテンツ復号鍵Ｋｃに対し、まず、ステップＳ２０５で生成されたKm［ＰＤＩＤ］（以下、これをｗと表す）を用いて暗号化を施す（ステップＳ２５２）。そして、ｗで暗号化されたコンテンツ復号鍵Ｋｃ（ｗ［Ｋｃ］）をステップＳ２５１の相互認証処理（ＡＫＥ）にて生成した鍵情報ＫＴ１を用いてさらに暗号化を行ってから（ＫＴ１［ｗ［Ｋｃ］］）、ＰＤ１２へ転送する（ステップＳ２５３）。

【０１４８】ＰＤ１２では、ステップＳ２５１の相互認証処理（ＡＫＥ）にて生成した鍵情報ＫＴ１を用いて、転送されてきたＫＴ１［ｗ［Ｋｃ］］を復号してｗ［Ｋｃ］を得、これを秘匿領域へ格納する（ステップＳ２５４）。

【０１４９】コンテンツ情報Ｃは、図１６の場合と同様に、Ｋｃで暗号化してから（ステップＳ２５５）、ＰＤ１２を経由してＭＣ１３へ転送される（ステップＳ２５６）。

【０１５０】図２０に示したようなチェックアウト処理動作に対応する再生処理動作について、図２１を参照して説明する。なお、図２０と同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、図２１において、ＰＤ１２は、自身の秘匿領域に格納されている暗号化コンテンツ復号鍵ｗ［Ｋｃ］を同じく自身の秘匿デバイスＩＤ（ＳＰＤＩＤ＝ｗ）を用いて復号し、コンテンツ復号鍵Ｋｃを得ることができる（ステップＳ

２６１）。このコンテンツ復号鍵Ｋｃを用いてＭＣ１３から転送されてきた暗号化コンテンツＫｃ［Ｃ］を復号して、コンテンツＣを得ることができる（ステップＳ２６２）。そして、ＰＤ１２では、コンテンツＣをデコーダ１２ｈでデコードして、Ｄ／Ａ変換部１２１でデジタル信号からアナログ信号に変換し、ＭＣ１３に記録されていた複製コンテンツ（例えば音楽）を再生することができる。

【０１５１】図２０に示したようなチェックアウト処理動作に対応するチェックイン処理動作は、図１８、図１９の説明とほぼ同様で、異なるのは、図１８のステップＳ６０３、図１９のステップＳ６５５でＰＤ１２の秘匿領域から消去されるのは、鍵情報ＫＴ１ではなく、ｗ＝ＫＭ［ＭＩＤ］で暗号化されたコンテンツ復号鍵ｗ［Ｋｃ］であるという点である。

【０１５２】

【発明の効果】以上説明したように、本発明によれば、記録媒体に記録された複製コンテンツの消去が確実にしかも安全に行え、記録媒体に記録する複製コンテンツの数の管理が容易にしかも確実に行える。

【図面の簡単な説明】

【図１】本発明の実施形態に係る記憶媒体（メディア）に記憶できる複製コンテンツの数を規制するためのコンテンツ管理方法を用いた音楽コンテンツ利用管理システム（ＬＣＭ）の構成例を示した図。

【図２】メモリ領域の構成例を示した図。

【図３】記録再生装置（ＰＤ）の内部構成例を示した図。

【図４】３種類の記憶媒体の特徴を説明するための図。

【図５】メディアインタフェース（Ｉ／Ｆ）部の内部構成例を示した図。

【図６】チェックイン後の記憶媒体の記録内容を説明するための図。

【図７】ＬＣＭの秘匿領域に格納されている宿帳の記憶例を示した図。

【図８】相互認証方法の概略を説明するための図。

【図９】チェックイン／チェックアウト処理手順を説明するためのフローチャートで、メディアの種別を判別して、その種別に応じた処理を選択するまでの手順を示したものである。

【図１０】記録媒体の種別がレベル２の場合のチェックアウト時の手順を説明するための図。

【図１１】記録媒体の種別がレベル２の場合の再生時の手順を説明するための図。

【図１２】記録媒体の種別がレベル２の場合のチェックイン時の手順を説明するための図。

【図１３】記録媒体の種別がレベル２の場合のチェックイン時の他の手順を説明するための図。

【図１４】記録媒体の種別がレベル２の場合のチェックアウト時の他の手順を説明するための図。

【図１５】記録媒体の種別がレベル２の場合の再生時の他の手順を説明するための図。

【図１６】記録媒体の種別がレベル０の場合のチェックアウト時の手順を説明するための図。

【図１７】記録媒体の種別がレベル０の場合の再生時の手順を説明するための図。

【図１８】記録媒体の種別がレベル０の場合のチェックイン時の手順を説明するための図。

【図１９】記録媒体の種別がレベル０の場合のチェックイン時の他の手順を説明するための図。

【図２０】記録媒体の種別がレベル０の場合のチェックアウト時の他の手順を説明するための図。

【図２１】記録媒体の種別がレベル０の場合の再生時の他の手順を説明するための図。

【図２２】相互認証処理（ＡＫＥ）の処理動作について説明するための図。

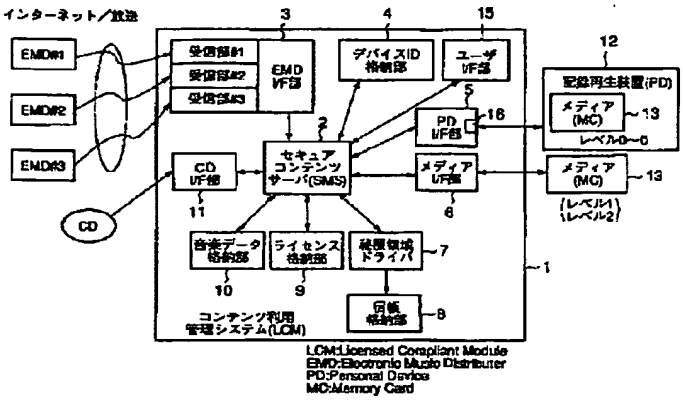
【図２３】相互認証処理（ＡＫＥ）の他の処理動作について説明するための図。

【図２４】図４（ｃ）に示したレベル２の記録媒体の構成をより具体的に示した図。

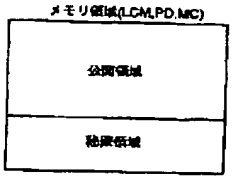
【符号の説明】

１…コンテンツ利用管理システム
２…セキュアコンテンツサーバ（ＳＭＳ）
３…ＥＭＤインタフェース部
４…タイムアウト判定部
５…ＰＤインタフェース（Ｉ／Ｆ）部
６…メディアインタフェース（Ｉ／Ｆ）部
７…秘匿領域ドライバ
８…宿帳格納部
９…ライセンス格納部
１０…音楽データ格納部
１１…ＣＤインタフェース（Ｉ／Ｆ）部
１２…記録再生装置（ＰＤ）
１３…記憶媒体（ＭＣ）

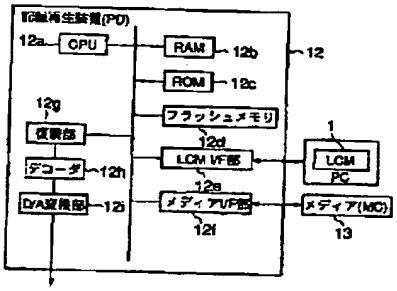
【図１】


インターネット／放送
EMD#1
EMD#2
EMD#3
CD
受信部#1
受信部#2
受信部#3
EMD I/F部
デバイスID 格納部
ユーザ I/F部
PD I/F部
記録再生装置(PD)
メディア (MC)
レベル0～0
セキュア コンテンツ サーバ(SMS)
CD I/F部
メディア I/F部
メディア (MC)
{レベル1 \レベル2
音楽データ 格納部
ライセンス 格納部
秘匿領域 ドライバ
領域 格納部
コンテンツ利用 管理システム(LCM)
LCM:Licensed Compliant Module
EMD:Electronic Music Distributer
PD:Personal Device
MC:Memory Card

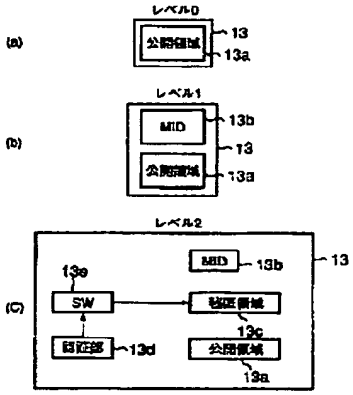
【図２】


メモリ領域(LCM,PD,MC)
公開領域
秘匿領域

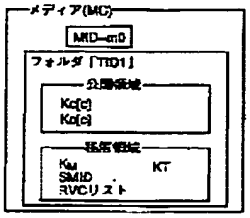
【図３】


記録再生装置(PD)
CPU
RAM
ROM
フラッシュメモリ
復号部
デコーダ
D/A変換部
LCM I/F部
メディアI/F部
LCM PC
メディア(MC)

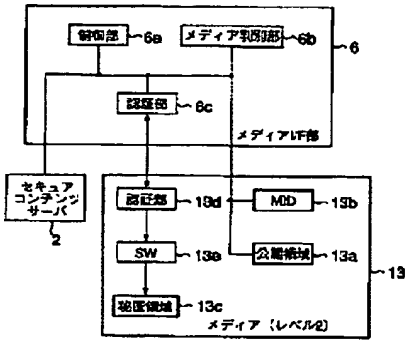
【図４】


(a)
レベル0
公開領域
(b)
レベル1
MID
公開領域
(c)
レベル2
MID
SW
秘匿領域
公開領域

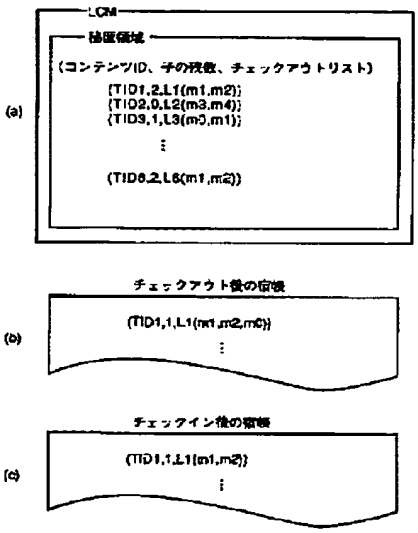
【図６】


メディア(MC)
MID=m0
フォルダ「TID1」
公開領域
Kc[c]
Kc[s]
秘匿領域
KM
KT
SMID
RVCリスト

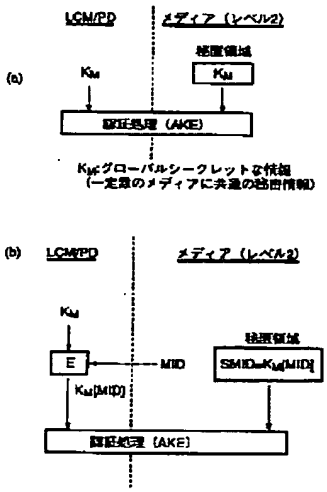
【図５】



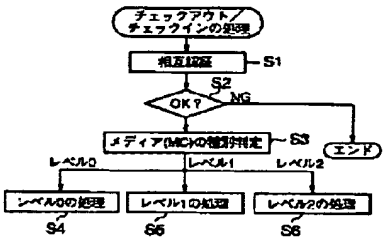
【図７】



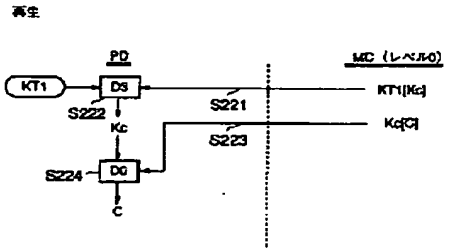
【図８】



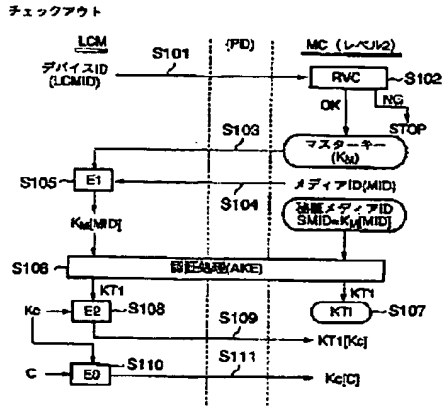
【図９】



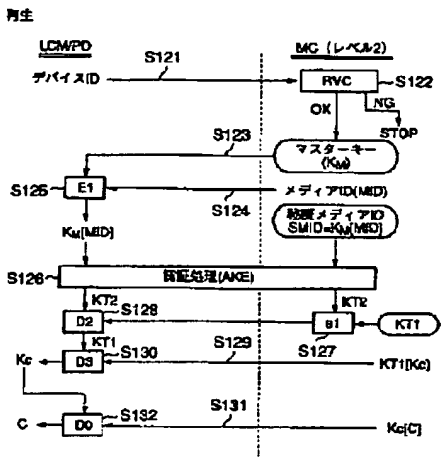
【図１７】



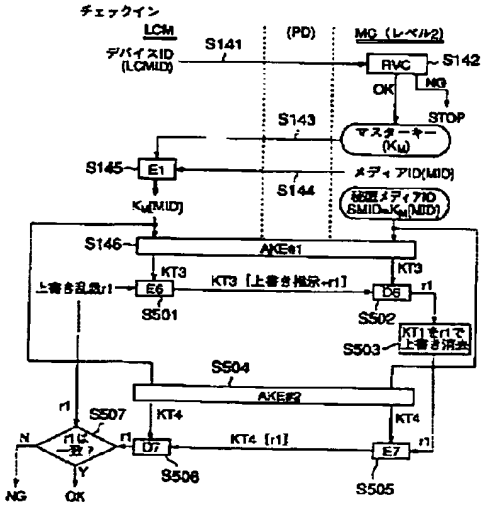
【図１０】



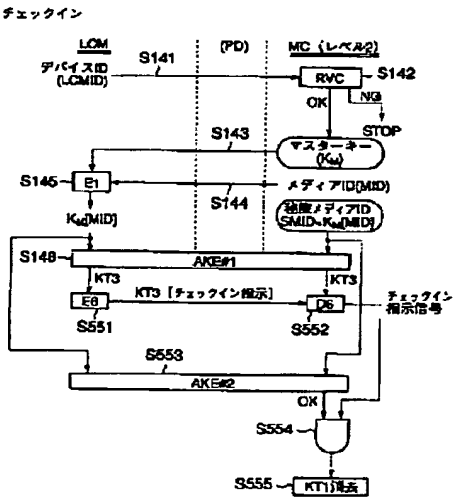
【図１１】



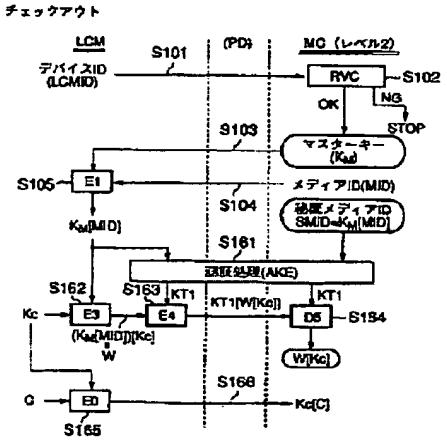
【図１２】



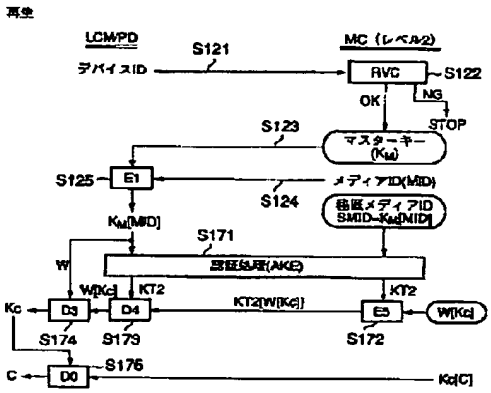
【図１３】



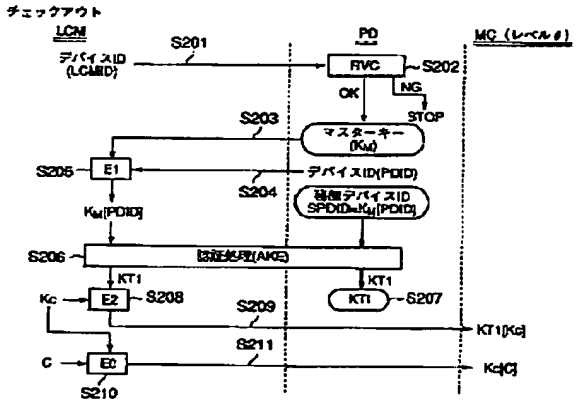
【図１４】



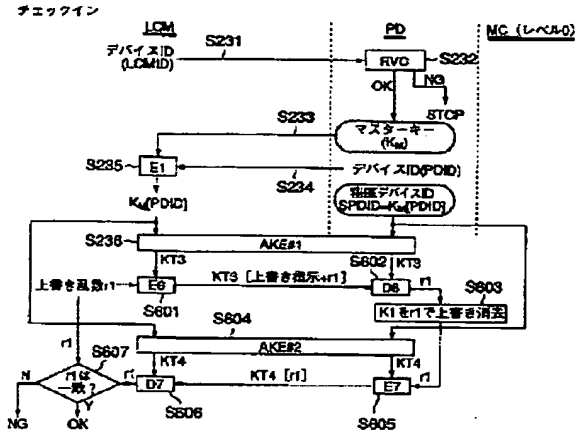
【図１５】



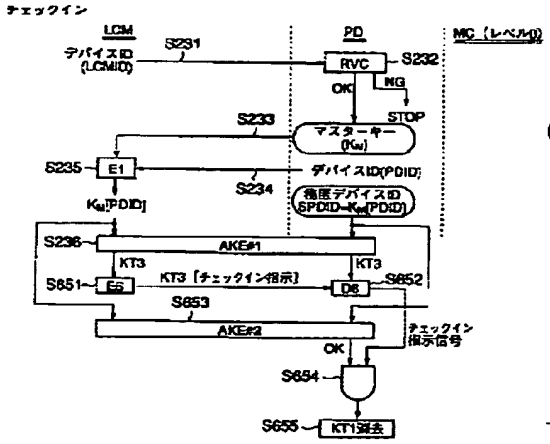
【図１６】



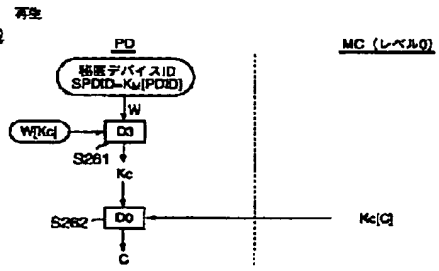
【図１８】



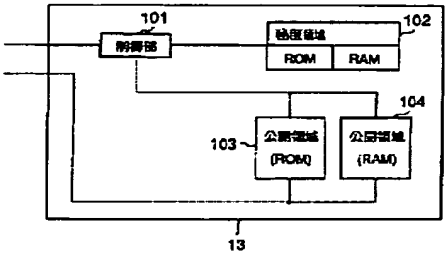
【図１９】



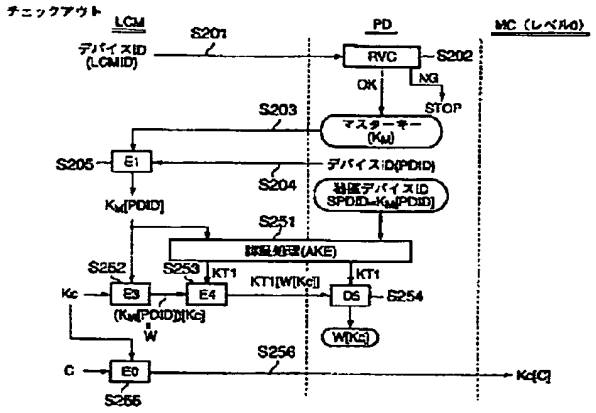
【図２１】



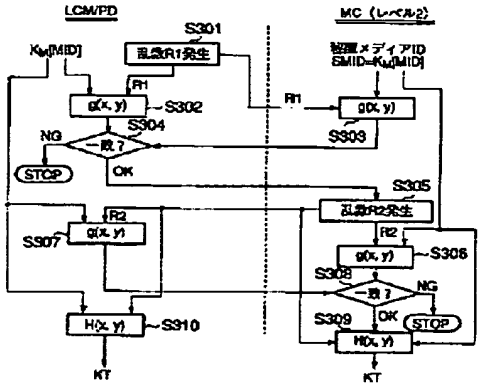
【図２４】



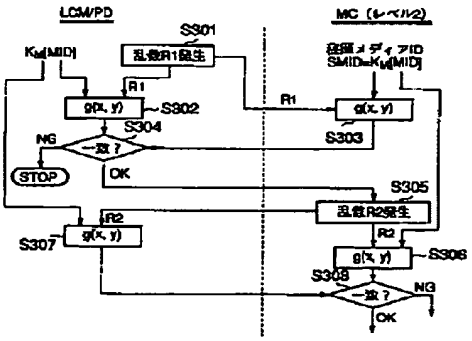
【図２０】



【図２２】



【図２３】



フロントページの続き

(72)発明者 加藤 拓
東京都府中市東芝町１番地 株式会社東芝府中工場内

(72)発明者 東間 秀之
東京都青梅市末広町２丁目９番地 株式会社東芝青梅工場内

(72)発明者 館林 誠
大阪府門真市大字門真1006番地 松下電器産業株式会社内

(72)発明者 草田 俊治
大阪府門真市大字門真1006番地 松下電器産業株式会社内

(72)発明者 山田 尚志
東京都港区芝浦一丁目１番１号 株式会社東芝本社事務所内

Ｆターム(参考) 5B017 AA06 BA05 BA07 BA08 BB02
CA08 CA09 CA14 CA15 CA16
5B085 AE23 AE29 CA04
5D044 AB05 DE50 GK11 GK17 HL11
5J104 AA07 BA03 KA01 NA27 PA05
PA07 PA14
9A001 BB03 BB04 EE03 EE04 LL03